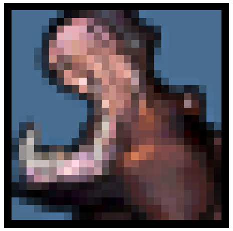
HIPAA PRIVACY TRAINING:
How to Build a Curriculum

Ann Dirks-Linhorst, Privacy Officer
Janet Conboy, HIPAA Project Coordinator
Ed Meyers, Security Officer
Missouri Department of Mental Health

Regional Provider Demonstrations
September, 2002

Today’s Agenda

- Review the key decisions and steps in building a privacy training that is HIPAA compliant
- Deconstruct and analyze one covered entity’s curriculum
- Discuss various approaches for initial and ongoing training, including new employee orientation
- Consider follow-up activities that support learning and culture change



Key Decisions and Steps

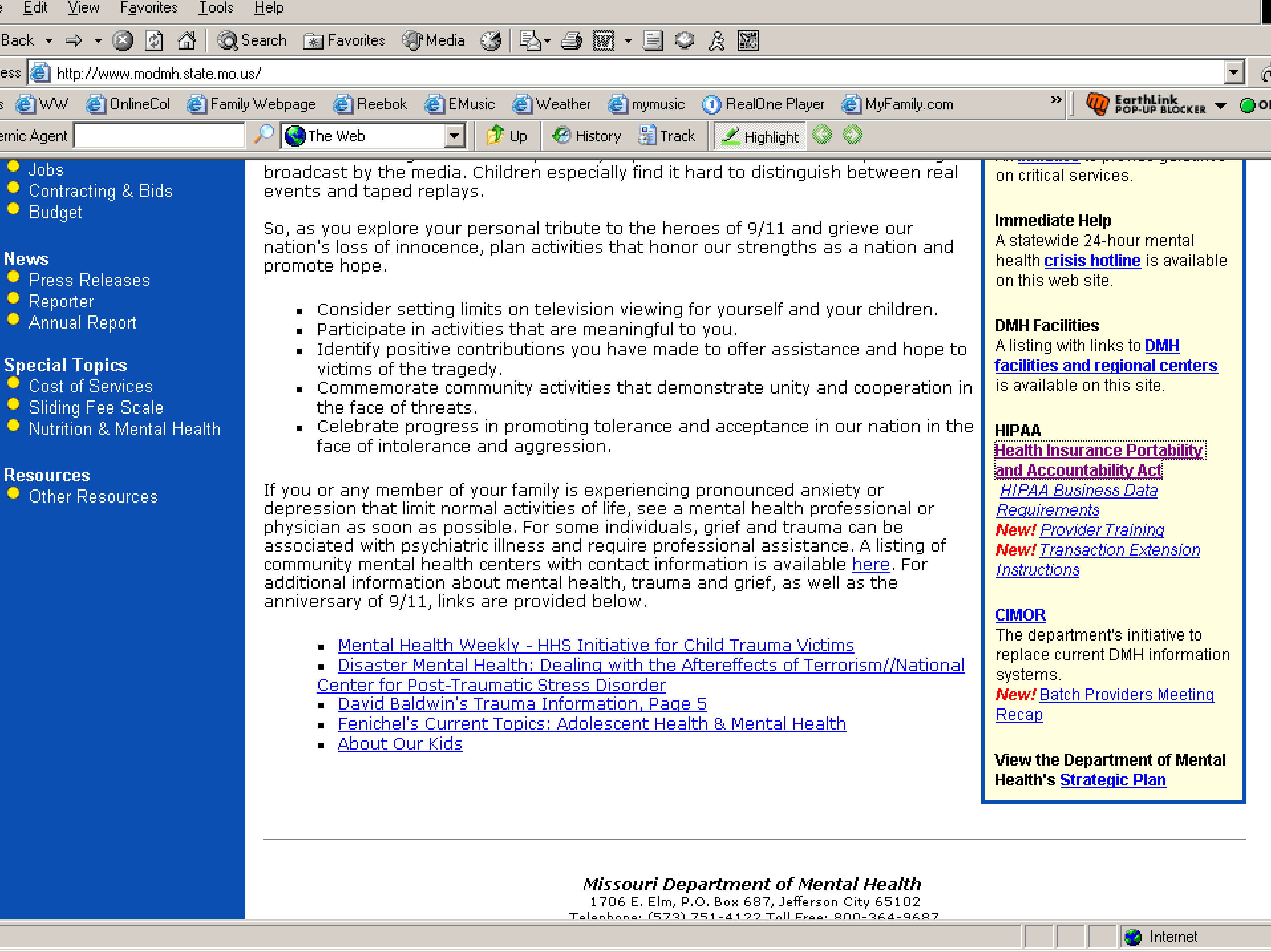
- Establish a core team
  - Education and Awareness Committee/Sponsor
- Conduct a privacy assessment
  - Pinpoint gaps in entity practice and policies
  - Identify barriers (resources, culture, existing contract requirements, security issues,etc.) to HIPAA compliance
  - Establish readiness benchmarks

Key Decisions and Steps

- Begin readiness campaign
    - Use the term “HIPAA” frequently
    - Conduct awareness sessions for key sectors of the organization
        - Leadership: Senior Management, Boards
        - Administration: Billing, Contracts, Facility Management
        - Clinical Services
        - Medical Records
        - Support (Maintenance, Housekeeping, Dietary)
        - Public Information
        - Business Associates/Trading Partners

Key Decisions and Step

- Begin readiness campaign
  - Establish a HIPAA page on your intranet and internet site
    - Updates to activities and policies
    - Assurance for staff and business associates of your commitment
    - Easy access to information about how HIPAA is being operationalized in your organization
    - Easy navigation



- Jobs
- Contracting & Bids
- Budget

News

- Press Releases
- Reporter
- Annual Report

Special Topics

- Cost of Services
- Sliding Fee Scale
- Nutrition & Mental Health

Resources

- Other Resources

broadcast by the media. Children especially find it hard to distinguish between real events and taped replays.

So, as you explore your personal tribute to the heroes of 9/11 and grieve our nation's loss of innocence, plan activities that honor our strengths as a nation and promote hope.

- Consider setting limits on television viewing for yourself and your children.
- Participate in activities that are meaningful to you.
- Identify positive contributions you have made to offer assistance and hope to victims of the tragedy.
- Commemorate community activities that demonstrate unity and cooperation in the face of threats.
- Celebrate progress in promoting tolerance and acceptance in our nation in the face of intolerance and aggression.

If you or any member of your family is experiencing pronounced anxiety or depression that limit normal activities of life, see a mental health professional or physician as soon as possible. For some individuals, grief and trauma can be associated with psychiatric illness and require professional assistance. A listing of community mental health centers with contact information is available here. For additional information about mental health, trauma and grief, as well as the anniversary of 9/11, links are provided below.

- Mental Health Weekly - HHS Initiative for Child Trauma Victims
- Disaster Mental Health: Dealing with the Aftereffects of Terrorism//National Center for Post-Traumatic Stress Disorder
- David Baldwin's Trauma Information, Page 5
- Fenichel's Current Topics: Adolescent Health & Mental Health
- About Our Kids

on critical services.

Immediate Help
A statewide 24-hour mental health **crisis hotline** is available on this web site.

DMH Facilities
A listing with links to **DMH facilities and regional centers** is available on this site.

HIPAA
Health Insurance Portability and Accountability Act
HIPAA Business Data Requirements
New! *Provider Training*
New! *Transaction Extension Instructions*

CIMOR
The department's initiative to replace current DMH information systems.
New! Batch Providers Meeting Recap

View the Department of Mental Health's Strategic Plan

Missouri Department of Mental Health
1706 E. Elm, P.O. Box 687, Jefferson City 65102
Telephone: (573) 751-4122 Toll Free: 800-364-9687

Key Decisions and Steps

- Training Parameters
  - Who is the target audience?
    - Staff/Board
    - Volunteers
    - Interns
  - What do they need to know?
    - Policies
    - Practice
    - Consumer interaction
    - Penalties
    - Gap-driven!

Key Decisions and Steps

- Training Parameters
  - What resources do you need to effect training?
    - In-house development? Off-the shelf? Customized?
    - Budget
    - Single or multiple sites?
    - Computer-based, traditional face-to-face or self-study paper-based?
    - Vendor availability?
    - Delivery: staff, media, space, time
    - How much time do you need to prepare and complete?
      - April 14, 2003 deadline
      - Driven by previous decisions
  - How are you going to document training compliance?

Key Decisions and Step

- Establish a training plan, with deliverables and timelines
- Get management sanction
- Deliver the goods!

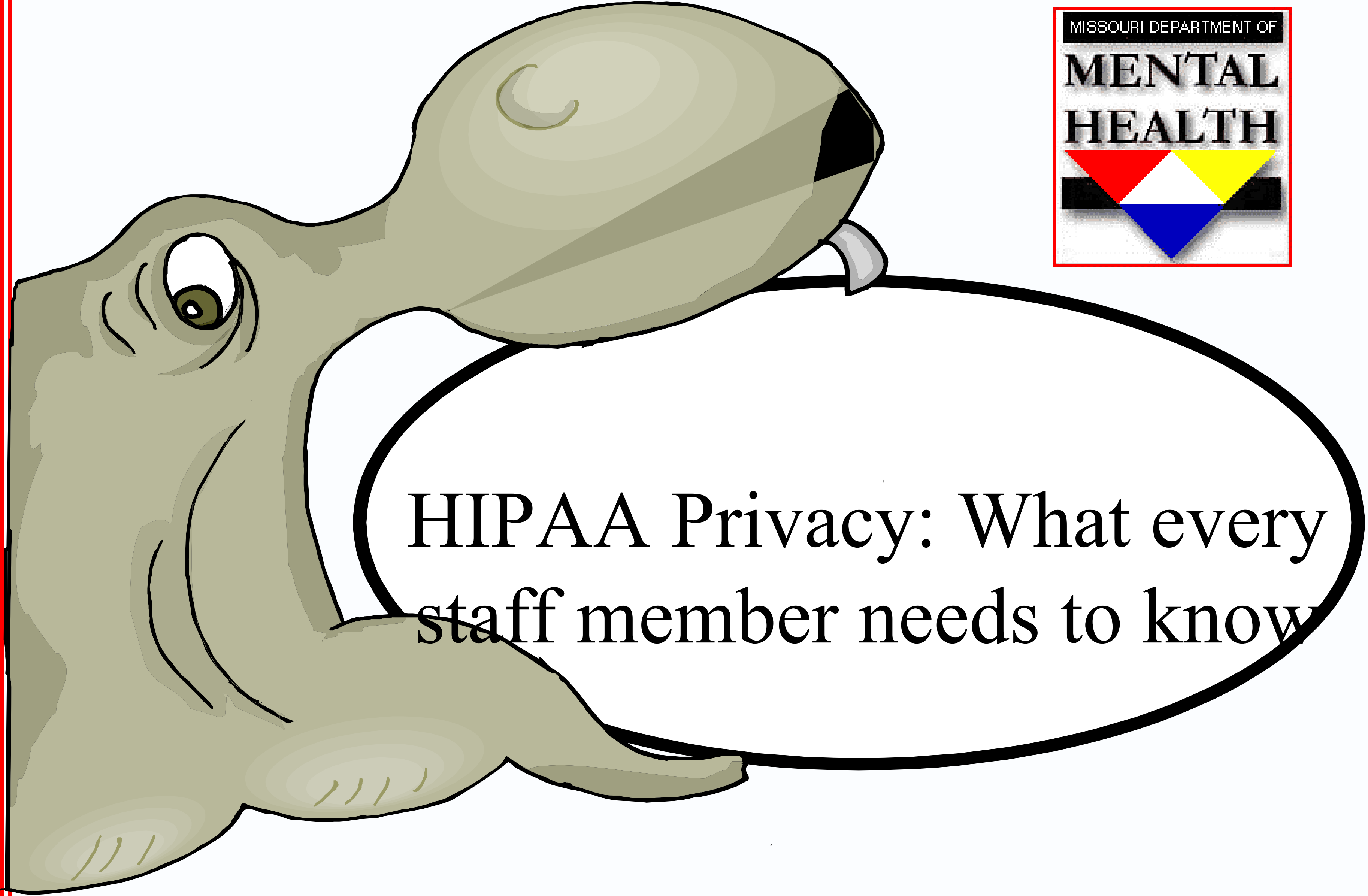
Deconstruct and Analyze One Covered Entity's Curriculum

- Missouri Department of Mental Health
  - 30 different facilities: large hospitals and small outpatient/case management agencies
  - 12,000 staff
  - Mental Health Commission
  - Few resources
  - Need to make consistent with business associate practices

Deconstruct and Analyze One Covered Entity’s Curriculum

- Use of SSM Video: “Hip to HIPAA”
- Decision to orient all staff at the same level
- Decision also made to conduct site-specific in-depth training with identified groups or individuals.

MISSOURI DEPARTMENT OF
MENTAL
HEALTH



HIPAA Privacy: What every staff member needs to know

Goals of Training

- To increase your knowledge & understanding of where **protected health information** is in this facility, and what threats may exist to its privacy and its security
- To enhance your awareness of **your role** in helping this facility follow HIPAA rules
- To provide information about to whom you can go with **questions** about privacy, and about security
- To inform you about your **reporting responsibilities** when HIPAA violations occur
- To alert you to the **possible penalties** for violation of HIPAA law for both you and this facility
- To protect the confidentiality of our consumer's PHI in support of one of our DMH values -- dignity, self-worth and individual rights. <u>It's the right thing to do!</u>

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996 – a Federal Law
  - Insurance Portability
  - Fraud Enforcement (Accountability)
  - Administrative Simplification
    - Privacy: **EFFECTIVE APRIL 14, 2003!!!**
    - Security (TBA)

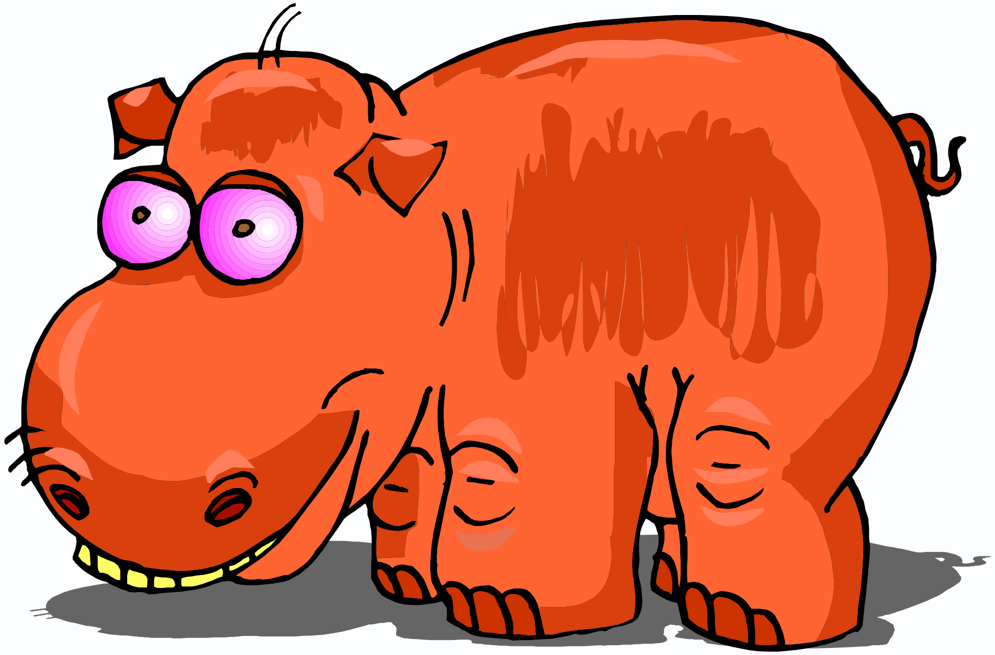
The DMH Service Delivery System is now an…

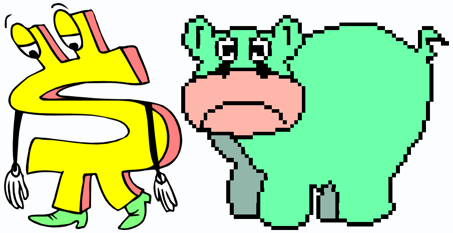
- ***Organized Health Care Arrangement***
  - Includes DMH and its contract providers
  - Addresses quality assessment and improvement
  - Allows information sharing using CIMOR – our new computer information system

HIPAA KEY TERMS

- Use
- Disclose
- Consent
- Authorization

Privacy
Why the concern?





HIPAA Enforcement

- **CIVIL PENALTIES**
  - $100 fine per person per violation
  - $25,000 fine per year for multiple violations
  - $25,000 fine cap per year per requirement.
  - *You* can be **personally** liable!

HIPAA Enforcement

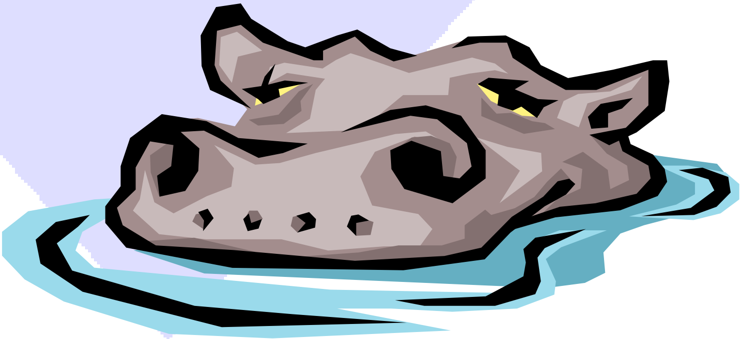
- **CRIMINAL PENALTIES**
  - Knowingly or wrongfully disclosing or receiving PHI: $50,000 fine and/or one year prison time
  - Commit offense under false pretenses:

    $100,000 fine and/or five years prison time
  - Intent to see PHI or client lists for personal gain or malicious harm:

    $250,000 fine and/or ten years prison time.
  - **Again, *you* can be *personally* liable!**

HIPAA Enforcement Continued

- These penalties apply to oral, paper and electronic information.
- **HIPAA also applies to you as a consumer of healthcare!**

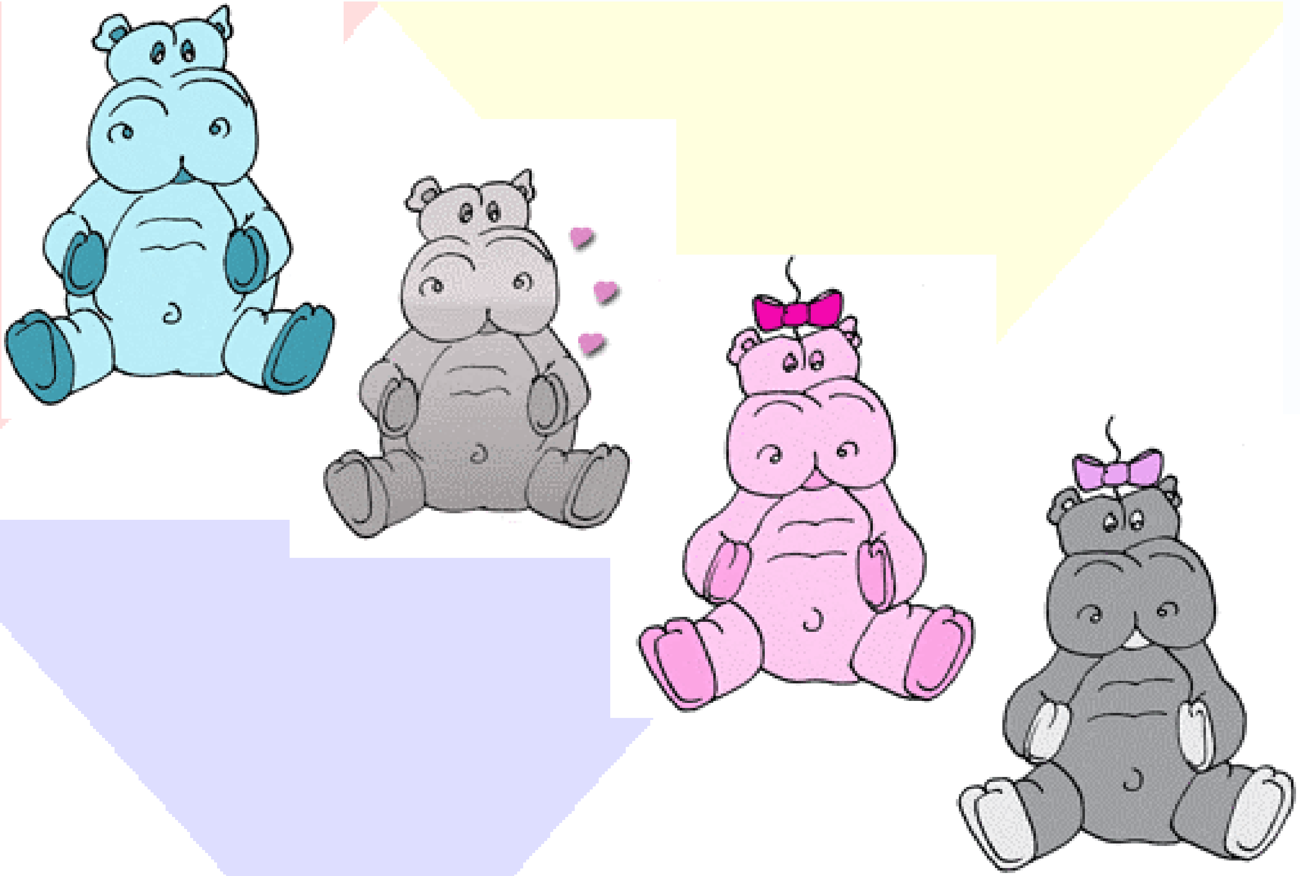


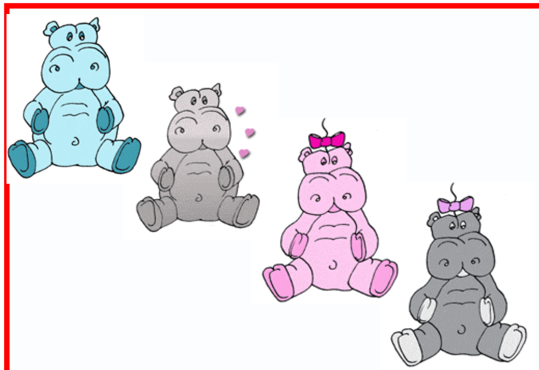
HIPAA Requires DMH to…..

- Establish or appoint
  - Policies and procedures to safeguard PHI
  - Privacy Officer
  - Security Officer
  - Privacy Officer and the Security Officer work with each facility’s HIPAA core team
  - Disciplinary actions policy

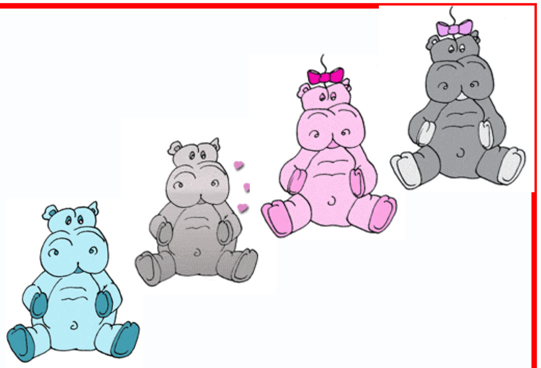
Examples of PHI

- 1. Name
- 2.
- 3.
- 4.
- 5.
- 6
- 7
- 8
- 9





Examples of PHI



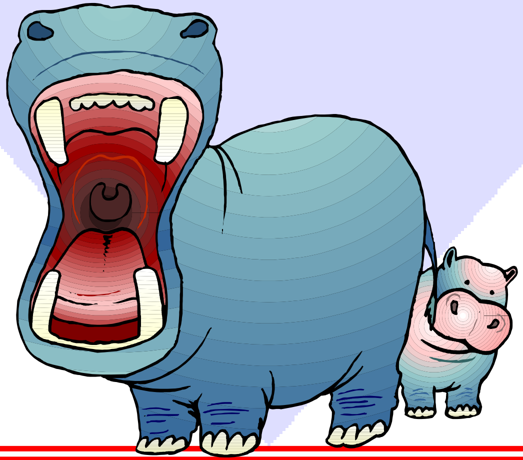
- Name/Address
- Employer
- Names of Relatives
- DOB/SSN
- Telephone number/
- Account number
- Occupation
- Diagnosis
- Treatment services and procedures

HIPAA Requires DMH to…..

- **Identify PHI Uses and Disclosures**
  - WHO:
    - People who routinely use or disclose (or receive requests to) PHI in our OHCA
  - WHAT:
    - Individually identifiable health information
  - HOW:
    - Written, oral, electronic communication

Challenge for DMH

- If you do **not** know *what or where* **PHI** is,
- and *who* uses or asks for it,
- You will be hard pressed to protect it.



Where do we find PHI?

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

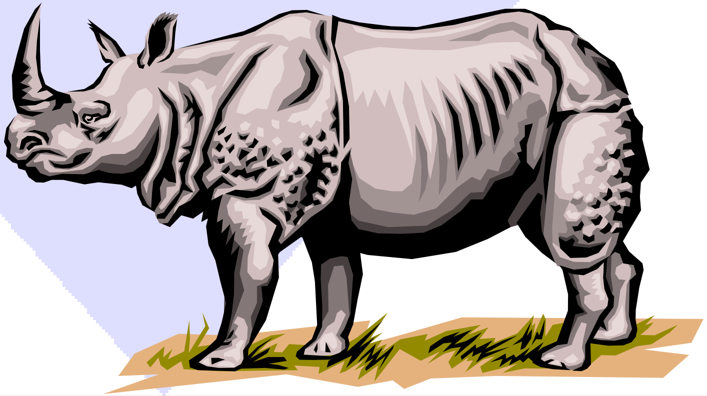
Where do we find PHI?

- Medical records and billing records
- Enrollment, payment
- Claims adjudication
- Case or medical management records

(Note---it exists both on paper and electronically)

PHI Does Not Include…..

- Thinks that aren't PHI:
  - Education records
  - Health information in your personnel record
  - Psychotherapy notes: (certain notes by mental health professionals/QMRPs)
    - Kept separate from the medical record, usually in a clinician's own file

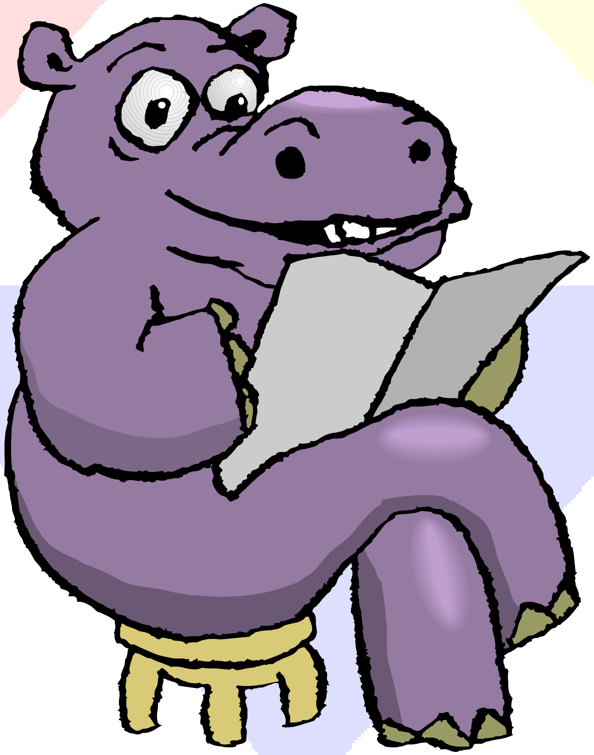


Psychotherapy Notes **ARE NOT**

- The following are not considered psychotherapy notes and therefore are PHI:
  - Medication prescription and monitoring
  - Counseling session start and stop times, the modalities and frequencies of treatment furnished
  - Clinical test results
  - Any summary of the following items: diagnosis functional status, the treatment plan, symptoms prognosis, and progress to date

Case Scenario Presentations

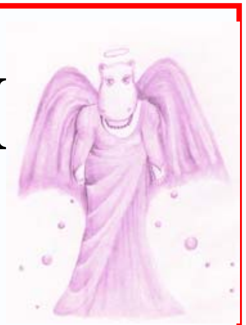
- How would we handle the following situations?



How Do Individual Staff Protect PHI? (Your List)

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

How Individual Staff Protect PHI (My List)



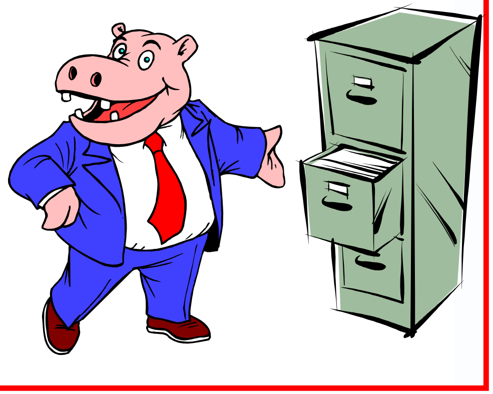
- Close doors or draw privacy curtains/screens
- Conduct discussions so that others may not overhear them
- Don’t leave medical records where others can see them or access them
- Keep medical test results private
- Don’t share PHI in public

WHETHER A HEALTH or FINANCIAL INTERVIEW, observe these guidelines!

Source: HCPro

Maintaining Records

- Safeguard PHI when records are in your possession
- Return medical records to appropriate location
- Dispose of paper consumer information properly

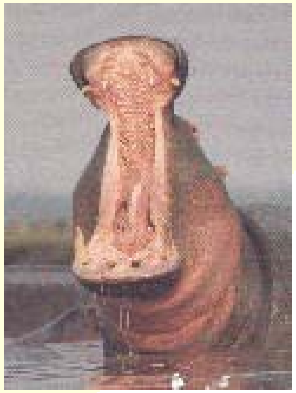


Source: HCPro

“Need to Know” Principles

- Necessary for your job
- How much do you need to know?
- How much do other people need to know?

How Does "Need to Know" Translate into HIPAA?

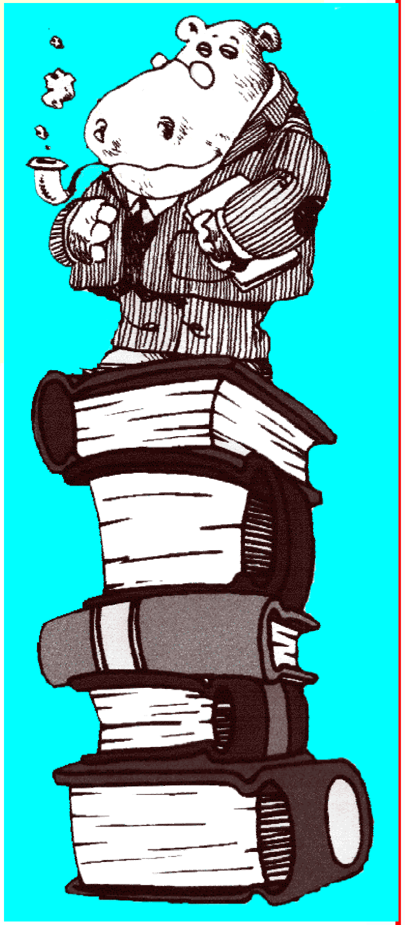


- **"Minimum necessary"** standard
  - Must provide only PHI
    - in the minimum necessary amount
    - to accomplish the purpose for which use or disclosure is sought
  - Minimum necessary does **not** apply when consumer executes valid authorization
  - New DOR

Privacy DORs

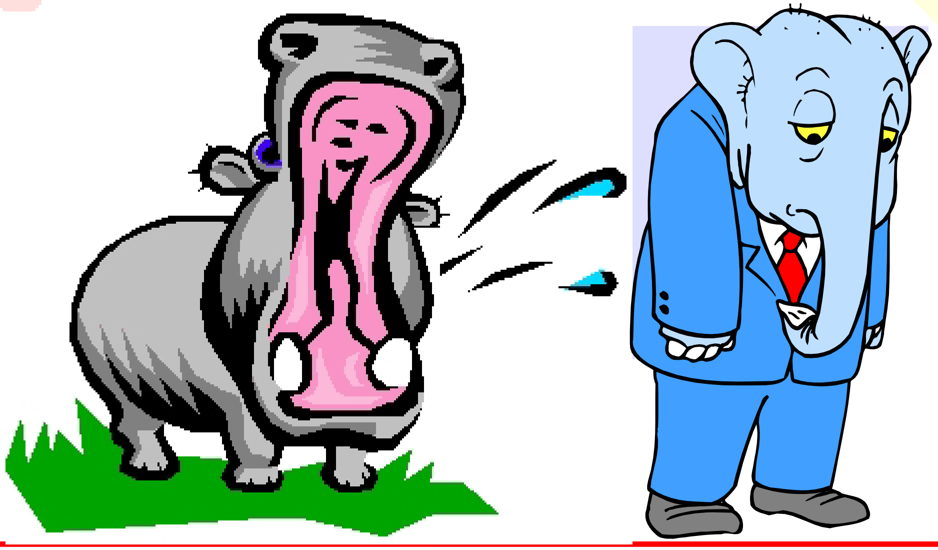
(Or How DMH Operationalizes The HIPAA Standards)

- HIPAA-related Department Operating Regulations are located in Chapter 8
- DORs can also be found at **dmhonline**



Privacy DORs

- Failure to follow/comply with the DORs **will** result in disciplinary actions
- KEY ACTIVITY: audit and monitoring



HIPAA DORs

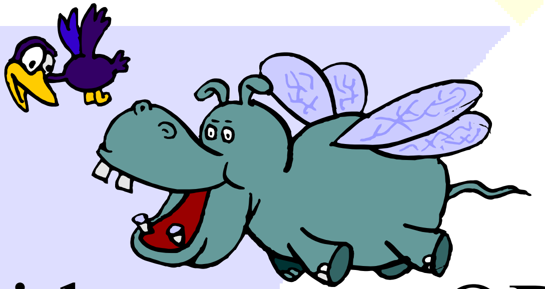
- Notice of Privacy Practices (8.005)
- Consumer Amendment of PHI (8.010)
- Restrictions (8.020)
- Access (8.030)
- Staff Access to PHI (8.040)
- Authorization to Disclose (8.050)
- Accounting of Disclosures (8.060)
- Verification (8.070)
- Field Practices (8.080)
- Training (8.090)

HIPAA Requires…

- **Notice of Privacy Practices (DOR 8.005)**
  - *Purpose*: to provide consumer with adequate notice of uses or disclosures of PHI
  - Must be written in plain language
  - Must be provided at the time of first service or assessment for eligibility
  - Has to provide Privacy Officer contact information
- All of DMH uses the same Notice

HIPAA Consumer Protections

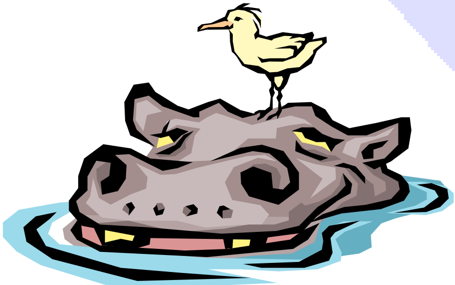
- **Amendment (DOR 8.010)**
  - Consumers may request to amend PHI in medical records
  - That request may be made to the facility Privacy Officer



- DMH facility may either *grant* OR *deny* the request

HIPAA Consumer Protections

- **Restrictions (DOR 8.020)**
  - Consumers may request that the facility *restrict* how it uses/discloses their PHI
  - Facility is NOT required to accept the request
  - <u>If restriction is accepted, then follow it</u>
    - Don’t deviate or depart from that restriction!

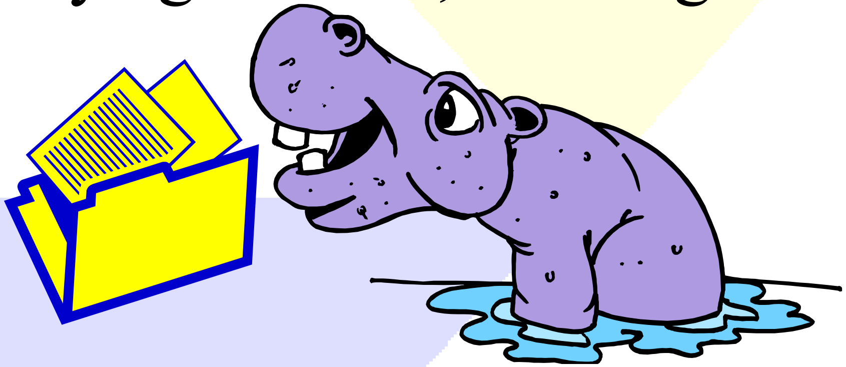


HIPAA Consumer Protections

- **Access (DOR 8.030)**
  - Consumers can access PHI
    - Inspect
    - Copy
  - Request for access MUST be in writing
    - Directed to the facility Privacy Officer
  - *If access is denied*, reason for that denial will determine if the consumer can appeal
  - Consumer must appeal to facility Privacy Officer

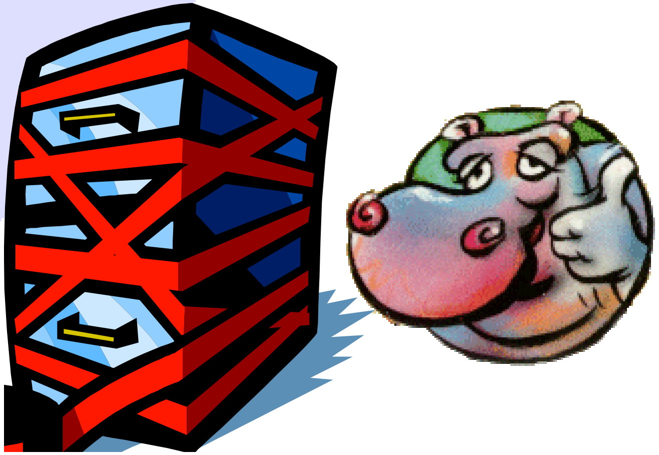
HIPAA PHI Protections

- **Staff Access to PHI (DOR 8.040)**
  - *Purpose*: to guide staff in keeping PHI confidential
  - Required confidentiality agreement, with signature of
    - Staff
    - Students
    - Volunteers
    - Visitors
  - <u>Inappropriate access of consumer PHI results in disciplinary action, possible other penalties</u>.



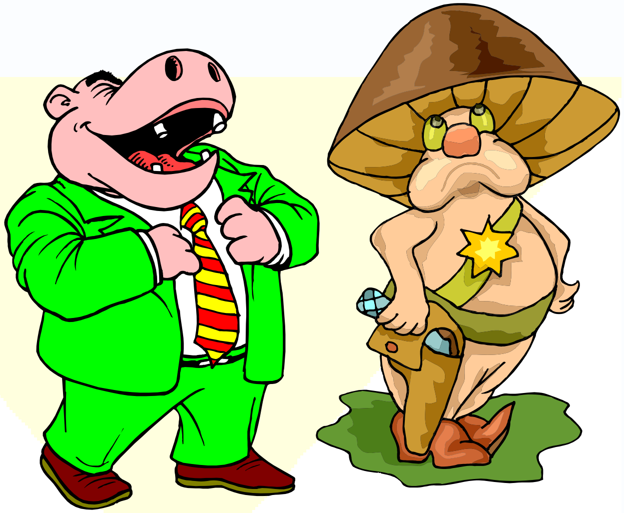
HIPAA Disclosure Protections

- **Authorization (DOR 8.050)**
  - Required to disclose PHI to person or agency outside the facility, DMH or the OHCA
  - Must be specific:
    - What PHI is to be shared
    - With whom
    - For what purpose
  - May be revoked



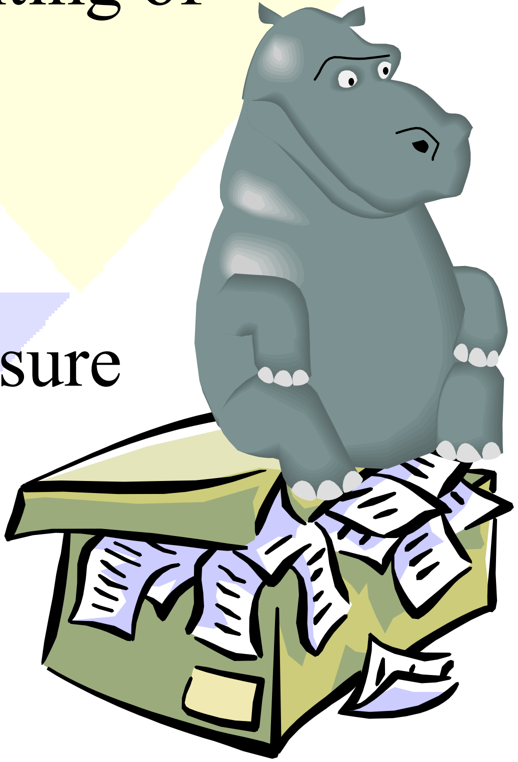
When No Authorization Is Needed…

- Key examples:
  - Child abuse/neglect reports
  - Judicial/administrative proceeding
  - Law enforcement
  - To avert serious threat to health or safety
  - Others



HIPAA Consumer Protections

- **Accounting of Disclosures (DOR 8.060)**
  - Consumers have a right for an accounting of disclosures
    - Time frame: 6-year period
    - Clock *starts*: April 14, 2003
  - Applies to both verbal and oral disclosure

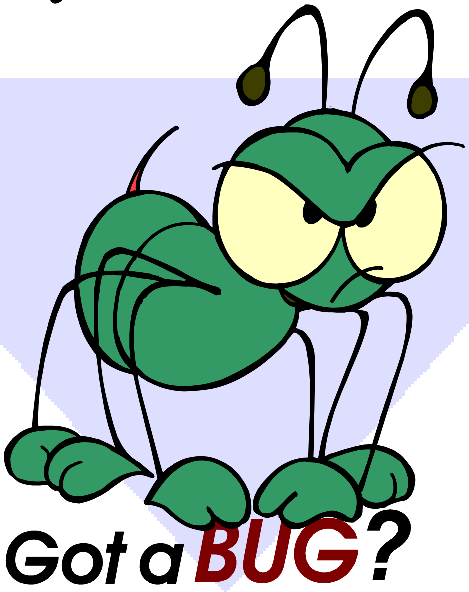


HIPAA Consumer Protections

- **Verification (DOR 8.070)**
  - Facility must verify that
    - Person or agency requesting the PHI
    - Is who they say they a
  - Facility must document the verification.

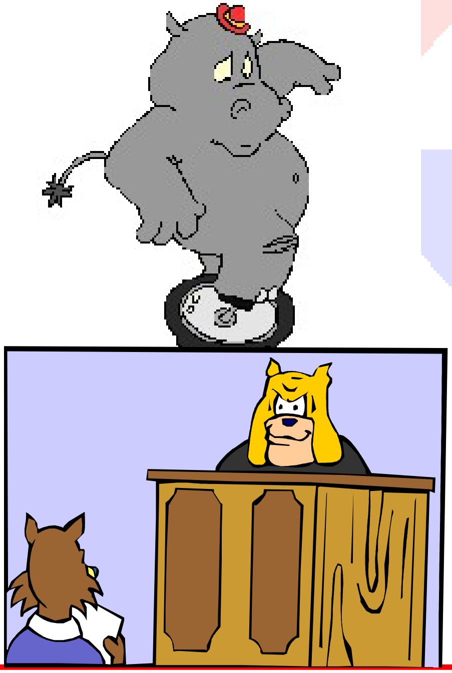
HIPAA Consumer Protections

- **Complaint Procedure**
  - HIPAA requirement
  - Allows a consumer to file a complain if they believe we have improperly used or disclosed their PHI



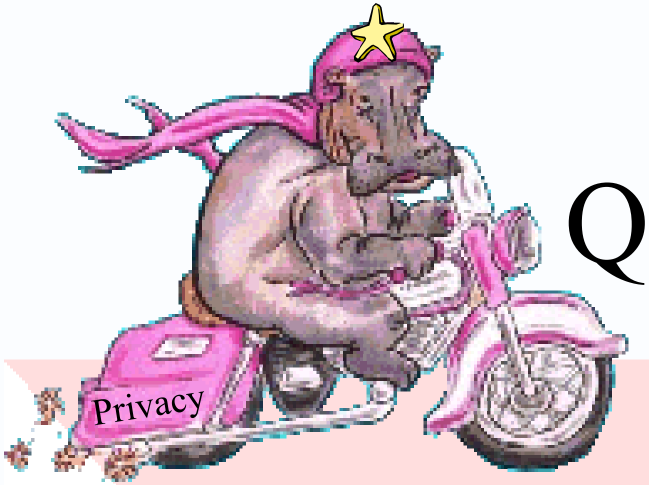
What Else Does HIPAA Require?

- **Preemption of state law**
  - Privacy Rule overrides any other state law **unless** that state law provides more protection for the consumer



WHAT ELSE DOES HIPAA REQUIRE?

- **Research**
  - HIPAA still allows research to be conducted
  - Proper authorizations must be in place



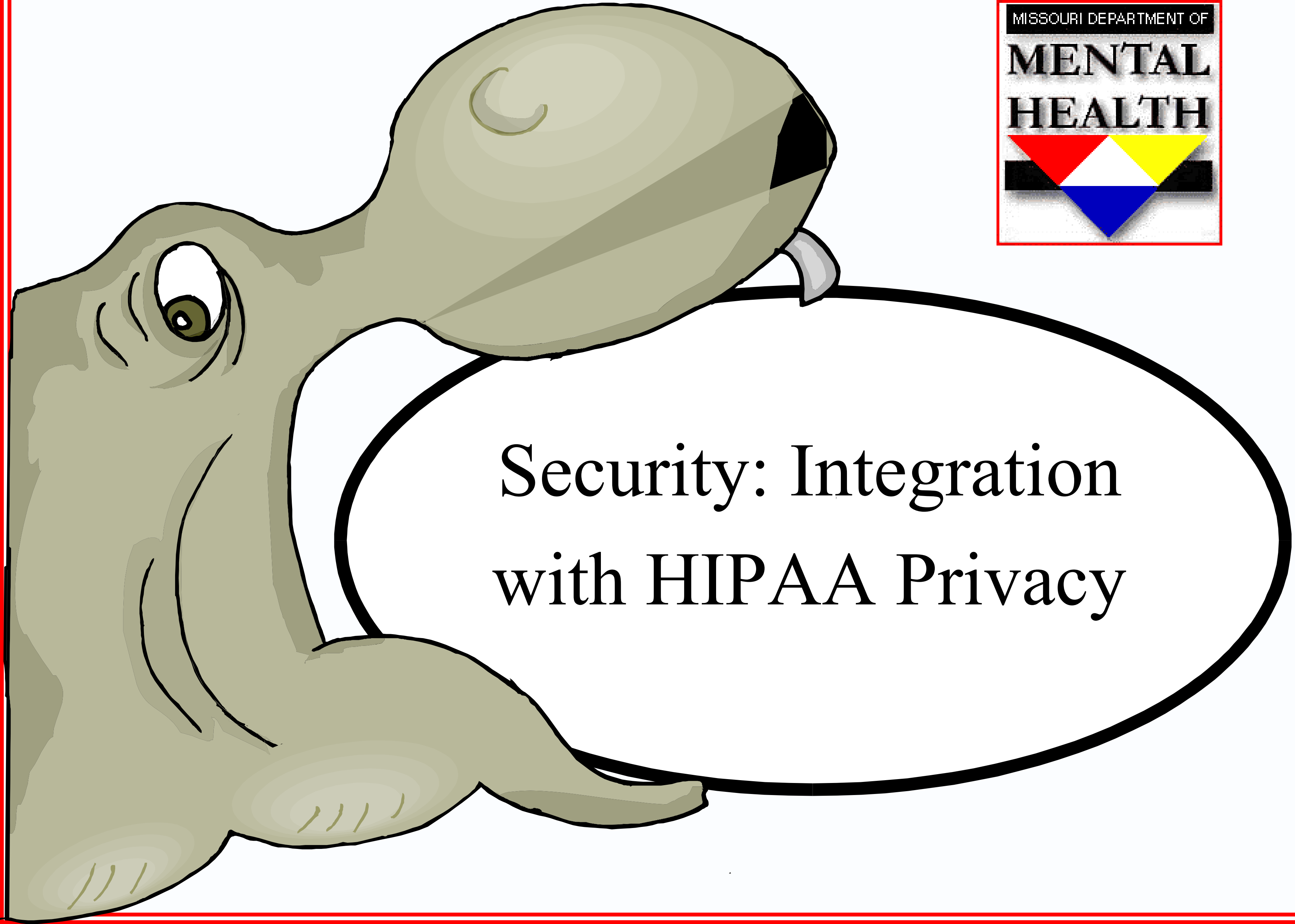
QUESTIONS?

- If you are ever in doubt, **always** ask your Privacy Officer or their designee!
- Remember, that person is your first line of response to privacy questions.

Key Things to Remember about Privacy

- We must safeguard consumer records
- Share only information necessary to do the work
- Consumers have the right to ask about use and disclosure of PHI
- DMH has DOR’s on HIPAA and you need to know them and follow them

MISSOURI DEPARTMENT OF MENTAL HEALTH



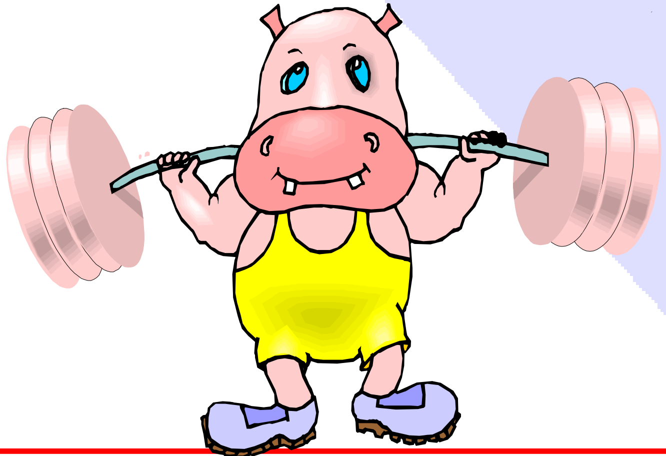
Security: Integration with HIPAA Privacy

Name that Password

- Just write down your answers to these questions
  - Your name
  - Spouse’s name
  - Child’s name
  - Birthday
  - Pet’s name
  - Street you live on
  - SSN

Required Training Areas

- Security Issues that Impact Privacy
  - General Security Awareness
  - System Access
  - Password Management



General Security Awareness

- Security (protecting the system and the information it contains) includes

  protecting against unauthorized access from outside and misuse from within

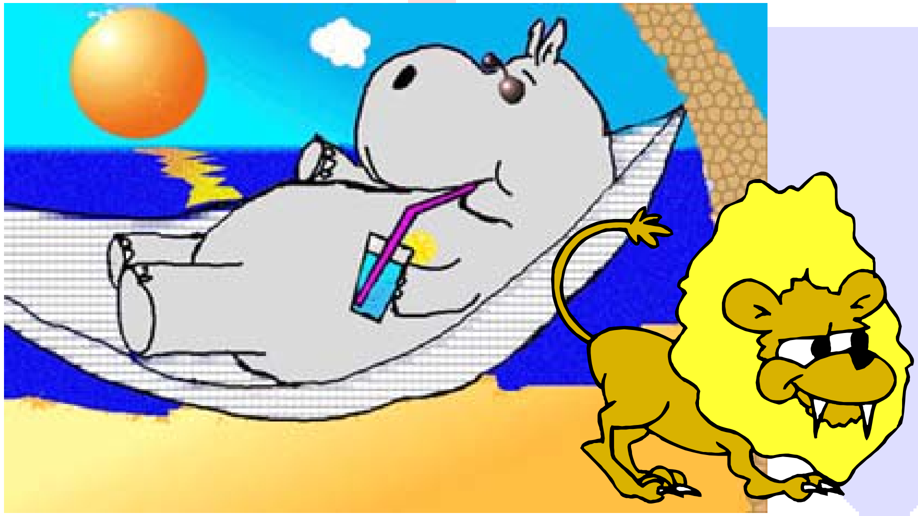
  - hardware and software,
  - personnel policies,
  - information practice policies,
  - disaster preparedness,
  - oversight of all these areas.

Purpose of Security

- To protect the system and information from unauthorized access
- To protect the system and information from unauthorized misuse

General Security Awareness

- Two Types of Security in HIPAA
  - Building\Physical Security
  - Computer\Electronic Security



General Security Awareness

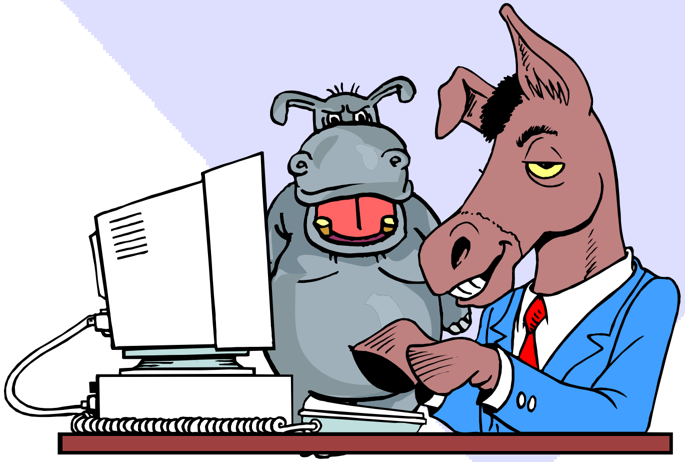
- Building\Physical Security
  - Building\Work Area Access
  - Locks and Keys
  - Badges\ID
  - Security Officer
  - Printers\Copy\Fax Machines

General Security Awareness

- Building\Work Area Access
  - Sign into building
  - Show ID\Visitors Badge
  - Patient\Client Area Entry

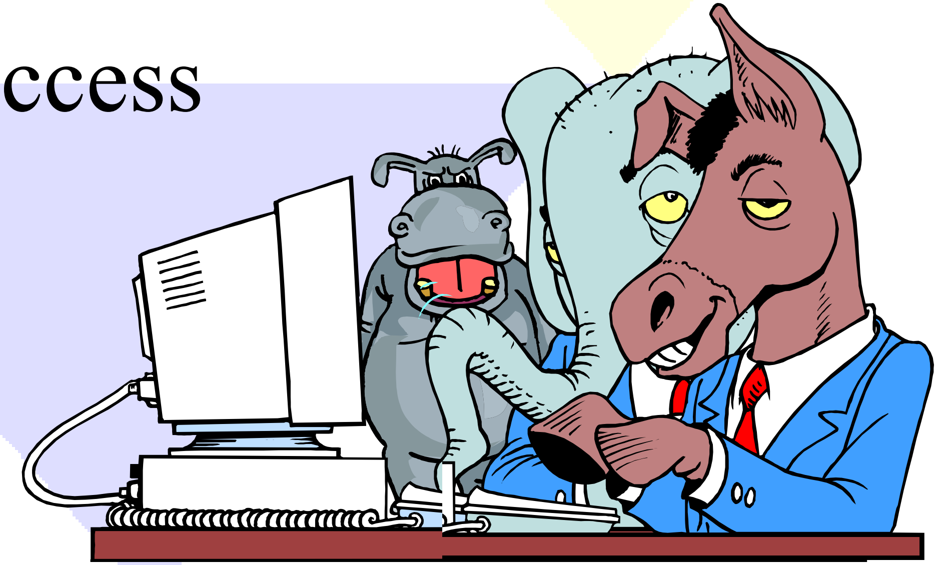
General Security Awareness

- Computer\Electronic Security
  - Computers
  - Location of PCs
  - Passwords\Log On
  - E-mail
  - Faxes

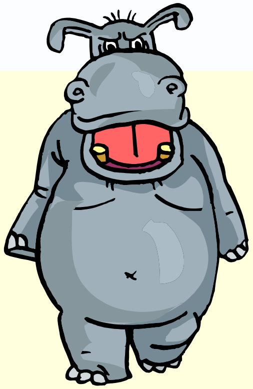


Things to Know about System Access

- Don’t share the session
- Report Discrepancies
- Be aware that disciplinary action may result
- Termination of Access



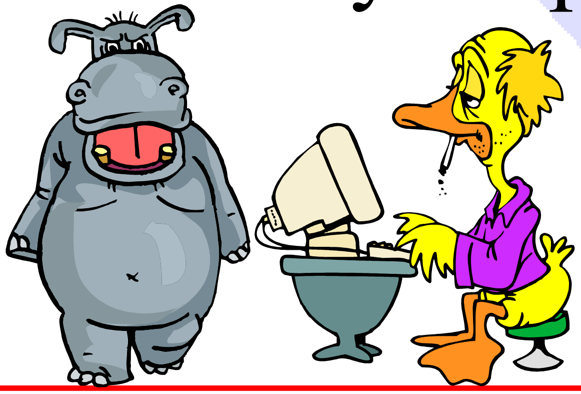
PC and System Protection



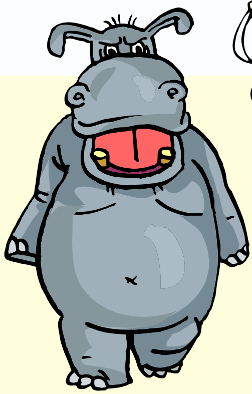
- Be aware of potential harm
- Follow the e-mail policy
- Don’t download non-DMH approved programs
- Report unknown or suspicious e-mail, attachments

Password Management

- What is Password Security?
  - Don’t tell anyone your password.
  - Don’t write your password down anywhere
  - Change password if others know it
  - Enter your password in private



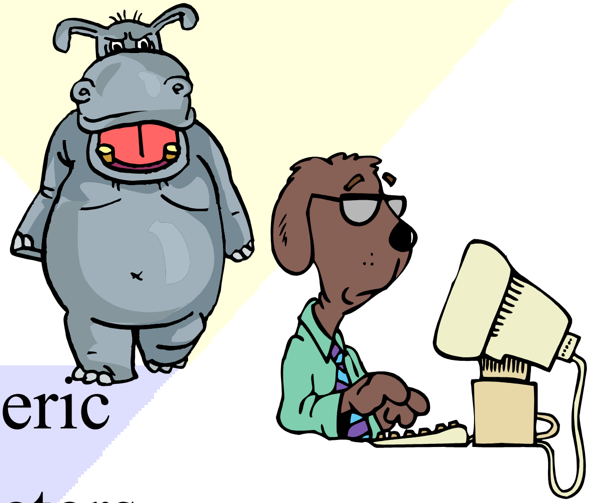
Password Management



- Guidelines for good passwords
  - **<u>Don’t</u>**
    - Choose password with more than 8 characters
    - Choose password that can be found in a dictionary
    - Choose password that uses public information such as SSN, Credit Card or ATM #, Birthday, date, etc.
    - Reuse old passwords or any variation
    - Use user id or any variation

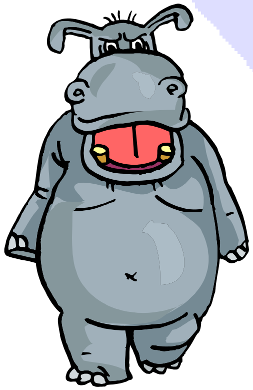
Password Management

- Guidelines for good passwords
  - **Do**
    - No clear link to you personally
    - Six to 8 characters
    - Minimum of 2 alpha and 1 numeric
    - Use upper and lower case characters
    - Change to a completely new password
    - Memorize your password



CIMOR's Role in Security

- Customer Information Management, Outcomes, and Reporting system
- Role will dictate access to CIMOR
  - Only access to what you need in order to do the job
- CIMOR will log all files access by specific user



CIMOR MENTAL HEALTH

Customer Information Management, Outcomes & Reporting

Key Things to Remember about Security

- Security impacts privacy
- Both building and computer security are important
- Fundamentals of good password management

Any Questions?

Approaches to Training

- Initial training for all staff
- New Employees

Follow-up to Training

- Focus on “It’s the Right Thing to Do”
- Move swiftly if corrective action is needed
  - Involve affected staff in problem-solving
  - Apply sanction if warranted
- Use intranet, newsletters, updates at meetings
- Keep it in front of all staff: posters, paycheck inserts, policy quizzes for prizes, HIPAA employee-of-the-quarter
- Frequent QA/QI reports to Board, Leadership